REMARKS

Claims 1-8, 28-29, and 31-34 are pending in the present application. By this Response, claims 1-4, 6-8, 28-29, and 31-33 are amended, claim 30 is canceled, and claim 34 is added. Independent claim 1 is amended to recite that the security information is inserted in a header of the object and that the determining and transmitting operations are performed at each device along the transmission path except for the target device. Independent claim 28 is amended similarly to recite the security information being in the header of the object and that the object is received only if the device provides the level of security required as specified in the header. The other claims are amended to be consistent with the amendments to their respective independent claims and for clarification purposes. Claim 34 is added to recite additional features of the invention. Support for the addition of claim 34 may be found at least at page 30, lines 9-12. Reconsideration of the claims is respectfully requested in view of the following remarks.

I. Telephone Interview

Applicants thank Examiner Gergiso for the courtesies extended to Applicants' representative during the July 21, 2009 telephone interview. During the telephone interview, the above amendments and the distinctions of the claims over the cited art were discussed. Examiner Gergiso indicated his understanding of the differences between the claimed invention and the cited references but stated that a more detailed review of the references was necessary before he would agree that the amended claims overcome the references. The substance of the telephone interview is summarized in the following remarks.

II. Claim Objections

The Office Action objects to claims 1, 2, 6, 9, 28, and 29 for various informalities. These claims are amended by this Response to address these informalities. Accordingly, Applicants respectfully request withdrawal of the objection to these claims.

III. Rejection under 35 U.S.C. § 103(a)

The Office Action rejects claims 1-8 and 28-33 under 35 U.S.C. § 103(a) as being allegedly unpatentable over Kaler et al. (U.S. Patent Application Publication No. 2004/0139322) in view of Lee IV et al. (U.S. Patent Application Publication No. 2005/0188072). This rejection is respectfully traversed.

A. Independent Claim 1

Independent claim 1 reads as follows:

> 1. A method, comprising:
> determining security information associated with a object of a transaction, ***wherein the security information is inserted in a header of the object*** and the object is to be transmitted from a source device to a target device along a transmission path that includes at least one intermediate device;
> determining, ***at each of the source device, and the at least one intermediate device along the transmission path as the object is transmitted along the transmission path, whether a next device in the transmission path to which the object is to be transmitted provides a level of security indicated by at least a portion of the security information in the header of the object***; and
> transmitting, ***at each of the source device, and the at least one intermediate device along the transmission path as the object is transmitted along the transmission path,*** the object to the next device in the transmission path ***in response to determining that the next device provides the level of security required by the at least a portion of the security information***.
> (emphasis added)

Applicants respectfully submit that the alleged combination of references fails to teach or render obvious at least those features of claim 1 emphasized above. The invention recited in claim 1 above operates on individual objects of a transaction and determines for the individual objects whether a next device in a transmission path to which the object is to be transmitted supports the required level of security identified in a portion of security

information in the header of the object. None of the cited references teach or render obvious such features.

Kaler is directed to a mechanism for establishing a secure context at ***communications end-points***. That is, Kaler is concerned with the two endpoint devices, i.e. the two ends source/target of the communications, negotiating secure context by transmitting portions of secure context back and forth between the two endpoints. The context is the set of mechanisms used to secure the data of a communication between the endpoints, which may include activating security mechanisms in communication protocol stacks operating at the two endpoints (see paragraph [0006]). At the first endpoint, a first application layer may determine that a first portion of context information is to be used to establish a secure context with a second application layer at a second endpoint. The context information is identified such that a secure context can be established between the first and second application layers independent of other context data identified at other layers in a communication stack (see paragraph [0016]). Similarly, the second endpoint may transmit a second portion of context information back to the first endpoint (see paragraph [0017]).

Thus, in Kaler, while a path from one endpoint to another may include intermediate devices, Kaler is only concerned with establishing the security mechanisms that are used at the endpoints of the communication, i.e. setting up the security mechanisms used in the protocol stacks at the endpoints. Kaler does not teach, or provide any technical rationale, to implement any security mechanisms in the intermediate devices along the way from the first endpoint to the second endpoint. Moreover, the establishment of the security mechanisms used by the endpoints is performed prior to any transmission of any data communications. That is, in Kaler, the security mechanisms are negotiated first so that the secure context is established and then communication using the secure context may be performed, i.e. the secure context must be established first and then transactions may be sent between the endpoints. This is primarily because Kaler is concerned with establishing different layers of security mechanisms independently of each other, such as at the application layer, the socket layer, etc.

To the contrary, with the invention as recited in claim 1, the security requirements are identified in header information of an actual object of a transaction. Thus, the

security requirements are determined from actual data that is being transmitted as part of an actual transaction. There is no need for an apriori establishment of a secure context. Nowhere in Kaler is there any teaching, or technical rationale, provided to include in the header of an object of a transaction, the security information identifying a level of security required to receive the object at a next device along a transmission path. Kaler mentions message headers in paragraphs [0078]-[0079] but does not teach the use of the header information to determine if a next device along a transmission path provides a required level of security and furthermore, does not teach that the message is an object of a transaction.

Moreover, the claimed invention determines at each device along a transmission path, whether the next device along the transmission path provides the required level of security identified in the header of the object. That is, rather than just establishing at the endpoints what the security mechanisms are that will be used to process communications at the two endpoints, the present invention ensures that each device along the transmission path provides a required level of security before the object is transmitted to that next device along the transmission path. Kaler does not teach, or provide any technical rationale, to implement such features. Kaler specifically states that it is the two endpoints that are establishing the secure context that they will each use. Such an approach as in Kaler leaves open a security hole that may be exploited as is described in the present application at page 4 because Kaler is a connection level security mechanism and not a transaction level mechanism. It is such a security hole that the present invention specifically cures by checking at each device whether the next device provides the level of security required by the security information in the header of the object being transmitted.

Thus, Kaler does not teach or render obvious at least the features of providing security information in a header of an object of a transaction or using, at each device along a transmission path from a source device to a target device, except for the target device, at least a portion of that security information to determine if a next device along the transmission path provides the level of security required by the portion of security information in the header of the object, and transmitting the object if the next device

provides the required level of security. Moreover, Applicants respectfully submit that Lee also fails to teach or render obvious these features.

Lee is directed to a mechanism for dynamically constructing a protocol to facilitate communication between nodes and across multiple nodes. Policies associated with the nodes are used to specify protocol properties of the nodes. A policy expression in a policy related to a node can be selected by another node to construct a protocol between the two nodes. A policy expression selection process can be applied to multiple nodes in a communication path to construct a protocol across the multiple nodes (see paragraph [0007]). A computer can retrieve an intermediate node policy characterizing communication properties supported by the intermediate node and may request destination node policies characterizing communication properties supported by a destination node (paragraphs [0009]-[0010]).

Yet again, with Lee, the protocol must be established first before any actual message communications are performed between a source and a destination. Lee provides a mechanism for establishing such a protocol dynamically based on the policies of the nodes between the source and destination. Essentially, the mechanism of Lee creates a protocol that is supported by all of the nodes along a communication path prior to performing any communication. This essentially means that the protocol that is created has a minimum number of protocol properties according to the lowest common denominator amongst the nodes.

Lee does not provide any teaching, or technical rationale, to implement the features of providing security information in a header of an object of a transaction, at least a portion of the security information identifying a required level of security required for each device along a transmission pathway, or using the portion of the security information at each device along the transmission pathway to determine if a next device along the pathway provides the required level of security and transmitting the object to the next device if the next device provides the required level of security. To the contrary, again, Lee is concerned with connection level protocol establishment, rather than providing a transaction level security mechanism, as is recited in claim 1. Lee is not concerned with performing security level checks on each individual device of a transmission path, whether the individual device provides a level of security required by

header information an object of a transaction prior to the object being transmitted to the device and transmitting the object to that device in response to a determination that the device supports the required level of security.

For the reasons set forth above, Applicants respectfully submit that neither Kaler nor Lee, either alone or in combination, teach or render obvious the features of claim 1. At least by virtue of their dependency on claim 1, the alleged combination of Kaler and Lee also fails to teach the features of dependent claims 2-8 and 31-33. Accordingly, Applicants respectfully request withdrawal of the rejection of claims 1-8 and 31-33 under 35 U.S.C. § 103(a).

B. Dependent Claims 2-8 and 31-33

In addition, dependent claims 2-8 and 31-33 recite additional features that are not taught or rendered obvious by the alleged combination of Kaler and Lee. For example, with regard to claim 2, the alleged combination of references fails to teach transmitting to the next device in the transmission path information representative of the level of security that is desired and receiving a response from the next device in the transmission path indicating that the next device in the transmission path provides the desired level of security. The Office Action alleges that these features are taught by Kaler at paragraph s [0049], [0110], and [0119]. These paragraphs of Kaler teach (1) what context information is (paragraph [0049]), (2) establishing a secure context from a first endpoint to a second endpoint by accepting context information sent from the first endpoint (paragraph [0110]), and (3) establishing a secure context from the second endpoint to the first endpoint by accepting context information sent from the second endpoint (paragraph [0119]). This does not teach sending information from a device to a next device in a transmission pathway identifying what level of security is desired and receiving a response that the other device provides that level of security. To the contrary, Kaler teaches one endpoint sending context information to the other endpoint and the other endpoint accepting it.

As a further example, regarding claim 6, the alleged combination of Kaler and Lee fails to teach or render obvious the features of determining an alternative device

along a different transmission path that provides the level of security required by the at least a portion of the security information in response to determining that the next device in the transmission path does not provide the level of security required by the at least a portion of the security information. The Office Action alleges that these features are taught by Lee at paragraph [0100] because this paragraph mentions that Lee "identifies any routing assertions." Here, the mechanism of Lee is stating that Lee determines if a node requires routing to another node, i.e. a routing assertion. This does not teach anything about determining an alternative device along a different transmission path ***that provides the level of security required*** by the at least a portion of the security information ***if the next device does not support the level of security required***. All that Lee is stating here is that if a node specifies another node to which it must route communications, Lee identifies that.

The other dependent claims recite additional features which, when taken alone or in combination with the features of independent claim 1, are not taught or rendered obvious by the alleged combination of references. Thus, dependent claims 2-8 and 31-33 are further distinguished over Kaler and Lee by virtue of the specific features recited in these claims.

C. Claims 28-29

Independent claim 28 recites similar subject matter to that of claim 1 in that independent claim 28 recites:

> 28. A method, comprising:
> receiving, at a first device along a transmission path from a source device to a target device, a request from a second device along the transmission path desiring to transmit an object to a third device, ***wherein the request includes at least a portion of security information associated with the object, the portion of security information being provided in a header of the object***;
> determining if the first device is adapted to provide a level of security ***identified by the at least a portion of security information in the header of the object***; and

transmitting an indication to the second device, ***based on determining if the first device provides the level of security identified by the at least a portion of security information***; and

receiving, in the first device, the object from the second device ***only in response to the first device transmitting an indication that the first device provides the level of security required by the at least a portion of security information***.

(emphasis added)

The inclusion of security information in a header of an object of a transaction as well as the use of such security information to determine whether to transmit the object to a next device in a transmission path has been addressed above. Similarly, claim 28 recites that security information in a header of an object that is to be transmitted along the transmission path is used to determine if a device to which the object is to be transmitted provides the level of security identified in the header and, only if it does, is the object received in the device to which the object is to be transmitted. For the reasons set forth above, Applicants respectfully submit that neither Kaler nor Lee, either alone or in combination, teach or render obvious such features. Claim 29 is dependent from claim 28 and is thus, distinguished over Kaler and Lee at least by virtue of its dependency. Accordingly, Applicants respectfully request withdrawal of the rejection of claims 28 and 29 under 35 U.S.C. § 103(a).

IV. Conclusion

It is respectfully urged that the subject application is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

Respectfully submitted,

DATE: July 23, 2009

Stephen J. Walder, Jr.
Reg. No. 41,534
WALDER INTELLECTUAL PROPERTY LAW, P.C.
17330 Preston Road, Suite 100B
Dallas, TX 75252
(972) 380-9475
ATTORNEY FOR APPLICANTS